Case Study: SECURITY CODE REVIEW

Objective	**Project**	▪ Client is a worldwide travel, financial and network services company and a much respected, popular brand in MENA region with presence in more than14 countries ▪ Client has 18 home grown applications to support their Cards function, which undergo frequent changes as per business requirement ▪ A periodic review is required to ensure any new changes or new application added to the stack is adhering to the security standards
	Challenges for Client	▪ The applications undergo frequent changes as per business requirement ▪ Applications have multiple interfaces with third party systems, which most of the time can't be controlled
	Challenges for Verinite	▪ Getting the code base for review / analysis on time ▪ The Applications are maintained by In-house staff. The teams maintaining these applications were changing frequently due to various reasons. Therefore, no uniform coding standards were followed ▪ Development of fixes suggested by Verinite took time due to resource unavailability at Client end. This had an impact on schedule for revalidation
Approach	▪ The security code review exercise was conducted for 18 custom applications using a combination of automated and manual review techniques. ▪ The review was done as per ➢ PCI-DSS requirements as put forth in clause 6.5 of the PCI-DSS v3.2 standards ➢ Secure Coding practices for applications put forth by OWASP Top 10 (Open Web Application Security Project) ➢ CERT Oracle Secure Coding practices for JAVA.Prepare documentation ▪ Verinite implemented a methodology comprising of following steps for a through and effective review ➢ Application Profiling ➢ Detailed Code walkthrough ➢ Threat Modelling ➢ Code Analysis ➢ Threat Analysis and reporting	
Value Delivered	▪ Verinite identified 328 vulnerability across 18 applications subjected to review ▪ Verinite suggested approach / code changes to fix these vulnerabilities ▪ Verinite re-evaluated the applications after these fixes were provided by Development team to ensure no high vulnerabilities were present	